

PATENT ABSTRACTS OF JAPAN

②

(11)Publication number : 11-167487

(43)Date of publication of application : 22.06.1999

(51)Int.Cl. G06F 9/06
G06F 13/00
G06F 13/00
G06F 15/00

(21)Application number : 09-331409

(71)Applicant : FUJITSU LTD

(22)Date of filing : 02.12.1997

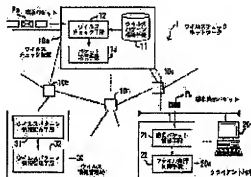
(72)Inventor : NOJIRI NATSUKI

(54) VIRUS CHECK NETWORK, VIRUS CHECK DEVICE, CLIENT TERMINAL AND VIRUS INFORMATION MANAGING STATION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a virus check network with improved efficiency to prevent viruses on a network side.

SOLUTION: A virus pattern housing means 11 houses virus patterns. A virus check means 2 executes virus check whether a packet is an infected packet Pa or not based on the virus patterns on the network side. At the time of detecting an infected packet Pa, a packet transmitting means 13 stands a bit showing infection within the packet and transmits it as an infection displaying packet Pb. An infected packet detecting means 21 detects the infected packet. A file execution control means 22 makes a file execution-disable corresponding to the infected packet. A virus pattern information delivering means 31 delivers virus pattern information to virus check devices 10a to 10n by multicasting. A virus pattern information managing means 32 uniformly manages virus pattern information.



(Partial Translation)

JP HE111-167487 A

5 [0013]

[Modes for carrying out the invention] Exemplary embodiments of the present invention are explained below with reference to the accompanying drawings. Fig. 1 is a principle diagram of a virus checking network according to the present invention.

10 [0014] The virus checking network 1 includes the virus checking units 10a to 10n, the client terminals 20a to 20m, and the virus information control base 30 to prevent intrusion of a virus by performing virus checking.

15 [0015] The virus pattern storing means 11 stores a virus pattern. The virus checking means 12 performs virus-checking whether a packet is an infected packet Pa by a virus on the network side by comparing between the received packet and a stored virus pattern.

20 [0016] When detecting the infected packet Pa, the packet transmitting means 13 sets a preset bit indicative of infection within the infected packet Pa and transmits it as an infection-indicated packet Pb.

[0017] The infection packet detecting means 21 detects is as the infection-indicated packet Pb based on the bit of the infection-indicated packet Pb. The file executing control means 22 disables executing of a file corresponding to the infection-indicated packet Pb.

[0018] The virus pattern information distributing means 31 distributes the updated virus pattern information to the virus checking units 10a to 10n by multicasting. The distributed virus pattern is stored by the virus pattern storing means 11.

[0019] The virus pattern information managing means 32

manages such as newly setting and updating of virus pattern information in an integrated fashion. The mode when the virus checking network 1 of the present invention is applied to a network on internet configured with routers, is explained below. The virus checking units 10a to 10n of the present invention are arranged in some of the routers to perform virus-checking on the network side.

[0020] Hereinafter, the router in which the virus checking unit is arranged is referred to as a virus checking router. Fig. 2 is a schematic view of a network on which virus checking routers are arranged. The network 1 includes routers R1 to R8, the client terminals 20a to 20m, and the virus information control base 30.

[0021] In the figure, the routers R1, R2, R3, and R4 are the virus checking router, and the other routers only have a general router function. The virus information control base 30 is connected to the virus checking router R2 and the client terminals 20a to 20m are connected to the virus checking router R4.

[0022] The portions (heading portion, middle portion, tailing portion) of the virus to be checked are shared among the virus checking routers R1 to R4 that are arranged so as to allow passing through each checking at least once.

[0023] Each of the virus checking routers R1 to R4 receives a virus pattern VP distributed by multicasting from the virus information control base 30, and stores always updated virus information.

[0024] The virus checking routers R1 to R4 compare the received packet with the stored virus pattern VP. If it is infected, a bit is set in the packet.

[0025] Concurrently, the warning packet Pw1 is returned to the source and the warning information packet Pw2 is distributed to each of the virus checking routers R1 to R4 by multicasting.

[0026] Each of the virus checking routers R1 to R4 that receives the warning information packet Pw2 performs priority detection of the virus or blocking the communication with the infection source. The client terminals 20a to 20m constantly monitor packets, and display a message to a user for alerting deletion of the received file when a bit indicative of infection is set or a packet is the warning packet Pw1.

10 [0059] Next, the warning packet Pw1 is explained. When the virus checking router detects a virus, the warning packet Pw1 is sent to the source and the warning information packet Pw2 is sent to the peripheral virus checking routers by multicasting, thereby enabling the

15 early finding of a virus and preventing the spreading thereof.

[0060] The warning packet Pw1 is set with a bit in the option area of the IP header similarly to the packet at the time of detecting a virus, to be distributed to the source

20 in the following format. Fig. 12 is a diagram illustrating a format of the warning packet Pw1. First, the IHL field is incremented by one. Then, the option area is set as The Copied flag=zero, The option Classes=three (area for future reservation), The option Number=two (code indicative of the

25 warning packet Pw1), length=three. Then, the option of the checking uncompleted/completed that is explained in Fig. 11 is added. The end address is the address of the infection source.

[0061] Next, processing on the client side is explained.

30 Fig. 13 is a diagram illustrating a configuration of a client terminal 20. The infection packet detecting means 21 of the present invention is included in a LAN driver 21a and the file executing control means 22 is included in a TCP/IP driver 22b.

[0062] The LAN driver 21a views a virus checking bit of each packet transmitted for each flow, determines whether a bit is set, and notifies the result to the TCP/IP driver 22b.

5 [0063] Upon receipt of notification that a bit is set, the TCP/IP driver 22b disables the execution of the corresponding file, and then displays a message 20-1 indicative of deleting the file.

[0064] Next, the flow of monitoring a bit at the client
10 terminal 20 is explained. Fig. 14 and Fig. 15 are flowcharts illustrating processing of monitoring a bit at the client terminal 20.

(S50) Read a packet.

(S51) Determine whether it is a new flow. If it is a new
15 flow, proceed to Step S52. If not, proceed to Step S53.

(S52) Add flow information.

(S53) Determine whether it is end of the flow. If it is the end of the flow, proceed to Step S54. If not, proceed to Step S55.

20 (S54) Delete the flow from the flow information.

(S55) Check the bit.

(S56) Determine whether being hit. In case of being hit, proceed to Step S58. If not, proceed to Step S57.

(S57) Hand over the processing to the TCP/IP driver 22b.

25 (S58) Determine whether it is the warning packet Pw1. In case of the warning packet, proceed to Step S59. If not, proceed to Step S60.

(S59) Display a message indicative of warning.

(S60) Nullify execution authority of the file.

30 (S61) Display the warning message 20-1.

[Brief description of the drawings]

[Fig. 1] A principle diagram of a virus checking network according to the present invention.

[Fig. 2] A schematic view of a network on which virus checking routers are arranged.

[Description of the numerals]

- 5 1 virus checking network
- 10a-10n virus checking units
- 11 virus pattern storing means
- 12 virus checking means
- 13 packet transmitting means
- 10 20a-20m client terminals
- 21 infection packet detecting means
- 22 file executing control means
- 30 virus information control base
- 31 virus pattern information distributing means
- 15 32 virus pattern information managing means
- Pa infected packet
- Pb infection-indicated packet
- VP virus pattern
- Pw1 warning packet
- 20 Pw2 warning information packet
- R1-R4 virus checking routers
- R5-R8 routers

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-167487

(43) 公開日 平成11年(1999)6月22日

(51) Int.Cl.⁵

識別記号

F I

G 0 6 F 9/06

5 5 0

G 0 6 F 9/06

5 5 0 Z

13/00

3 5 1

13/00

3 5 1 Z

3 5 5

3 5 5

15/00

3 3 0

15/00

3 3 0 A

審査請求 未請求 請求項の数12 O L (全 14 頁)

(21) 出願番号

特願平9-331409

(22) 出願日

平成9年(1997)12月2日

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 野尻 夏樹

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

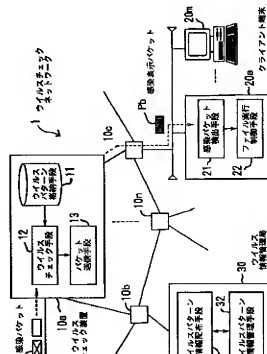
(74) 代理人 弁理士 服部 毅彦

(54) 【発明の名称】 ウィルスチェックネットワーク、ウィルスチェック装置、クライアント端末及びウィルス情報管理
理局

(57) 【要約】

【課題】 ネットワーク側でウィルスを未然に防ぎ、ウィルス対策効率の向上を図ったウィルスチェックネットワークを提供することを目的とする。

【解決手段】 ウィルスパターン格納手段11は、ウィルスパターンを格納する。ウィルスチェック手段12は、パケットをウィルスパターンにもとづいて、感染パケットPaか否かのウィルスチェックをネットワーク側で行う。パケット送信手段13は、感染パケットPaを検知時は、パケット内の感染を示すビットを立てて感染表示パケットPbとして送信する。感染パケット検出手段21は、感染パケットPaを検出する。ファイル実行制御手段22は、感染パケットに対応するファイルを実行不可にする。ウィルスパターン情報配布手段31は、ウィルスパターン情報をマルチキャストでウィルスチェック装置10a～10nに配布する。ウィルスパターン情報管理手段32はウィルスパターン情報を一元管理する。



【特許請求の範囲】

【請求項1】 ウィルスチェックを行って、ウィルス侵入を防止するウィルスチェックネットワークにおいて、ウィルスパターンを格納するウィルスパターン格納手段と、受信したパケットを前記ウィルスパターンにもとづいて、ウィルスに感染している感染パケットか否かの前記ウィルスチェックをネットワーク側で行うウィルスチェック手段と、前記感染パケットを検出した場合は、感染を示すパケット内のビットを立てて感染表示パケットとして送信するパケット送信手段と、から構成される複数のウィルスチェック装置と、

前記ビットにもとづいて、前記感染パケットを検出する感染パケット検出手段と、前記感染パケットに対応するファイルを実行不可にするファイル実行制御手段と、から構成されるクライアント端末と、ウィルスパターン情報をマルチキャストで前記ウィルスチェック装置に配布するウィルスパターン情報配布手段と、前記ウィルスパターン情報を一元管理するウィルスパターン情報管理手段と、から構成されるウィルス情報管理局と、を有することを特徴とするウィルスチェックネットワーク。

【請求項2】 前記ウィルスチェック手段は、前記パケットのヘッダを見て前記ウィルスチェックすべき前記パケットを選定することを特徴とする請求項1記載のウィルスチェックネットワーク。

【請求項3】 前記ウィルスチェック装置は、ルータに配置されることを特徴とする請求項1記載のウィルスチェックネットワーク。

【請求項4】 前記ウィルスチェック装置は、前記ウィルスパターン情報を前記マルチキャストで互いに通知することを特徴とする請求項1記載のウィルスチェックネットワーク。

【請求項5】 前記ウィルスチェック装置は、前記ウィルスの脅威レベルに応じて警戒モードを設定し、ホストとの通信を一定時間遮断させる警戒モード設定手段をさらに含むことを特徴とする請求項1記載のウィルスチェックネットワーク。

【請求項6】 前記ウィルスチェック装置は、前記ウィルスチェックを行う部位を複数設け、前記ウィルスチェック装置毎に担当するウィルスチェック領域を分担することを特徴とする請求項1記載のウィルスチェックネットワーク。

【請求項7】 前記ウィルスチェック装置は、ネットワーク上新規に置かれた場合は、他の前記ウィルスチェック装置から前記ウィルスチェックの担当領域情報を収集することを特徴とする請求項6記載のウィルスチェックネットワーク。

【請求項8】 前記ウィルスチェック装置は、前記感染パケットを検出した場合は、対応するファイルを実行不可にするファイル実行制御手段と、を有することを特徴するウィルスチェック装置。

告パケットを送信し、かつ他の前記ウィルスチェック装置に警戒すべき前記感染パケットの情報が記された警戒情報パケットをマルチキャストで配布することを特徴とする請求項1記載のウィルスチェックネットワーク。

【請求項9】 前記ウィルスチェック手段は、前記警戒情報パケットに記された前記感染パケットの前記ウィルスパターン情報の優先順位を上げて、前記ウィルスチェックを行うことを特徴とする請求項8記載のウィルスチェックネットワーク。

【請求項10】 ウィルスチェックを行って、ウィルス侵入を防止するウィルスチェック装置において、ウィルスパターンを格納するウィルスパターン格納手段と、

受信したパケットを前記ウィルスパターンにもとづいて、ウィルスに感染している感染パケットか否かの前記ウィルスチェックをネットワーク側で行うウィルスチェック手段と、前記感染パケットの場合は、感染を示すパケット内のビットを立てて感染表示パケットとして送信するパケット送信手段と、

を有することを特徴するウィルスチェック装置。

【請求項11】 ウィルスチェックを受けたパケットを受信するクライアント端末において、ウィルスに感染されていることを示すビットが立っているパケットを感染パケットとして検出する感染パケット検出手段と、

前記感染パケットを検出した場合は、対応するファイルを実行不可にするファイル実行制御手段と、を有することを特徴するクライアント端末。

【請求項12】 ネットワーク内のウィルス情報を管理するウィルス情報管理局において、ウィルスパターン情報を前記ネットワーク内に配置されたウィルスチェックを行うウィルスチェック装置にマルチキャストで配布するウィルスパターン情報配布手段と、前記ウィルスパターン情報を一元管理するウィルスパターン情報管理手段と、を有することを特徴するウィルス情報管理局。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はウィルスチェックネットワーク、ウィルスチェック装置、クライアント端末及びウィルス情報管理局に関し、特にウィルスチェックを行って、ウィルス侵入を防止するウィルスチェックネットワーク、ウィルスチェックを行って、ウィルス侵入を防止するウィルスチェック装置、ウィルスチェックを受けたパケットを受信するクライアント端末及びネットワーク内のウィルス情報を管理するウィルス情報管理局に関する。

【0002】

信ネットワーク技術が急速に進歩している。また、インターネット等の流行により、企業のみならず一般家庭に対しても、ネットワークが提供するサービスが幅広く利用されている。

【0003】この反面、コンピュータウィルスの増加と感染のスピードは、ネットワークの普及と共に加速しており、多くの企業ユーザがウィルスの被害に遭っている現状が報告されている。

【0004】従来、ネットワークをウィルスの感染から守るには、クライアントやプロキシサーバ等にワクチン・ソフトを導入していた。このワクチン・ソフトを用いることにより、ウィルスに感染しているファイルからウィルスを取り去って、ファイルを修復することができ

る。

【0005】「発明が解決しようとする課題」しかし、上記のような従来のウィルス対策は、クライアント側で行っているため、感染防止にはクライアントすべてに対して、個々にワクチン・ソフトを導入しなければならない。

【0006】このため、新種ウィルスに対しては、バージョンアップしたワクチン・ソフトを最初から逐一導入しなければならず、時間が非常にかかり効率が悪いといった問題があった。

【0007】また、従来のクライアント側でのウィルス対策では、新種ウィルス発見時のパターンファイルの更新などをはじめとする運用管理等は、各自ユーザに任せられるため、ウィルス監視を徹底させることが難しいといった問題があった。

【0008】本発明はこのような点に鑑みてなされたものであり、ネットワーク側でウィルスを未然に防ぎ、ウィルス対策効率の向上を図ったウィルスチェックネットワークを提供することを目的とする。

【0009】また、本発明の他の目的は、ネットワーク側でウィルスを未然に防ぎ、ウィルス対策効率の向上を図ったウィルスチェック装置を提供することである。さらに、本発明の他の目的は、ウィルスに感染しているファイルを削除して、ウィルス対策効率の向上を図ったクライアント端末を提供することである。

【0010】また、本発明の他の目的は、ネットワーク内のウィルス情報を管理して、ウィルス対策効率の向上を図ったウィルス情報管理局を提供することである。

【0011】

【課題を解決するための手段】本発明では上記課題を解決するために、図1に示すような、ウィルスチェックを行って、ウィルス侵入を防止するウィルスチェックネットワーク1において、ウィルスパターンを格納するウィルスパターン格納手段11と、受信したパケットをウィルスパターンにもとづいて、ウィルスに感染している感

Paを検知した場合は、感染を示すパケット内のビットを立てて感染表示パケットPbとして送信するパケット送信手段13と、から構成される複数のウィルスチェック装置10a~10nと、ビットにもとづいて、感染パケットPaを検出する感染パケット検出手段21と、感染パケットPaに対応するファイルを実行不可にするファイル実行制御手段22と、から構成されるクライアント端末20a~20mと、ウィルスパターン情報をマルチキャストでウィルスチェック装置10a~10nに配布するウィルスパターン情報配布手段31と、ウィルスパターン情報を一元管理するウィルスパターン情報管理手段32と、から構成されるウィルス情報管理局30と、を有することを特徴とするウィルスチェックネットワーク1が提供される。

【0012】ここで、ウィルスパターン格納手段11は、ウィルスパターンを格納する。ウィルスチェック手段12は、受信したパケットをウィルスパターンにもとづいて、ウィルスに感染している感染パケットPaが否かのウィルスチェックをネットワーク側で行う。パケット送信手段13は、感染パケットPaを検知した場合は、感染を示すパケット内のビットを立てて感染表示パケットPbとして送信する。感染パケット検出手段21は、ビットにもとづいて、感染パケットPaを検出する。ファイル実行制御手段22は、感染パケットに対応するファイルを実行不可にする。ウィルスパターン情報配布手段31は、ウィルスパターン情報をマルチキャストでウィルスチェック装置10a~10nに配布する。ウィルスパターン情報管理手段32は、ウィルスパターン情報を一元管理する。

【0013】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図1は本発明のウィルスチェックネットワークの原理図である。

【0014】ウィルスチェックネットワーク1は、ウィルスチェック装置10a~10nと、クライアント端末20a~20mと、ウィルス情報管理局30と、から構成され、ウィルスチェックを行って、ウィルス侵入を防止する。

【0015】ウィルスパターン格納手段11は、ウィルスパターンを格納する。ウィルスチェック手段12は、受信したパケットと、格納してあるウィルスパターンと、を比較し、パケットがウィルスに感染している感染パケットPaが否かのウィルスチェックをネットワーク側で行う。

【0016】パケット送信手段13は、感染パケットPaを検知した場合は、感染パケットPa内のあらかじめ設定した感染を示すビットを立てて、感染表示パケットPbとして送信する。

【0017】感染パケット検出手段21は、感染表示パ

Paと検出する。ファイル実行制御手段22は、感染パケットPaに対応するファイルを実行不可にする。

【0018】ウイルスパターン情報配布手段31は、最新のウイルスパターン情報をマルチキャストでウィルスチェック装置10a～10nに配布する。配布されたウイルスパターンは、ウイルスパターン格納手段11で格納される。

【0019】ウイルスパターン情報管理手段32は、ウイルスパターン情報の新規設定、更新等の管理を一元的に行う。次に本発明のウィルスチェックネットワーク1を、ルータで構成されているインターネット上のネットワークに適用した場合の実施の形態について説明する。本発明のウィルスチェック装置10a～10nをいくつかのルータに配置させ、ネットワーク側でウィルスチェックを行う。

【0020】なお、ウィルスチェック装置を配置したルータを以降では、ウィルスチェックルータと呼ぶ。図2はウィルスチェックルータを配置したネットワークの概要を示す図である。ネットワーク1は、ルータR1～R8と、クライアント端末20a～20mと、ウィルス情報管理局30と、から構成される。

【0021】図ではルータR1、R2、R3、R4がウィルスチェックルータであり、その他は通常のルータ機能のみを持つ。ウィルスチェックルータR2にウィルス情報管理局30が接続し、ウィルスチェックルータR4にクライアント端末20a～20mが接続する。

【0022】ウィルスチェックルータR1～R4はウィルスのどの部分（先頭部、中間部、終端部）をチェックするかを分担させており、各担当を最低1回は通過するように配置させる。

【0023】各ウィルスチェックルータR1～R4は、ウィルス情報管理局30からマルチキャストで配布されるウイルスパターンVPを受け取り、常に最新のウィルス情報を保持しておく。

【0024】受信したパケットに対し、ウィルスチェックルータR1～R4は保持してあるウィルスパターンVPと比較する。もし感染している場合にはパケットにビットを立てる。

【0025】その際同時に送信元に対しては警告パケットPw1を返し、各ウィルスチェックルータR1～R4に対しては、警戒情報パケットPw2をマルチキャストで配布する。

【0026】警戒情報パケットPw2を受け取った各ウィルスチェックルータR1～R4は、そのウィルスを優先的に検出、あるいは感染元との通信の遮断を行う。クライアント端末20a～20mでは、パケットを常に監視しており、感染を示すビットが立っている場合、あるいは警告パケットPw1だった場合にはユーザにメッセージを出力し、感染防止のための対応を促す。

ウィルスパターンVPは、マルチキャストにのせて定期的に配布される。また新種のウィルスが発見されたら、ウィルス情報管理局30は新たに作成したウィルスパターンVPをマルチキャストで各ウィルスチェックルータ10a～10nに送り、各ウィルスチェックルータ10a～10nは変更があればウィルスパターンを更新する。

【0028】図3はウィルスパターンVPのフォーマットを示す図である。ウィルスパターンVPは、ヘッダVP-1にEther HeaderとIP Header(Multicast)とを持つ。そして、ウィルスパターン配布を示すコードVP-2と、ウィルスの種類を示すシリアル番号VP-3と、そのバージョン（改版番号）VP-4を持つ。

【0029】これらのあとに、実際のウィルスのバイナリから先頭部分（第1領域のウィルスパターン）VP-6、中間部分（第2領域のウィルスパターン）VP-7、終端部分（第3領域のウィルスパターン）VP-7を固定長バイトごと抽出したものを付ける。

【0030】なお、抽出部分はウィルス情報管理局30によって任意に決められ、定期的に更新してバージョンVP-4を更新する。また、ウィルスの危険度に応じて脅威レベルVP-5をウィルス情報管理局30で決定しておく。これにより危険度に応じた対応を可能にする。

【0031】ウィルスチェックルータ10a～10nでは、受け取ったデータを元に自分の持つウィルスパターンVPを後述の検索テーブルに追加する。その際、各ウィルスチェックルータ10a～10nはどの領域を分担するか決められており、受信したパケットから自分の担当するパターンのみを受け取る。

【0032】次にウィルスパターンVPの格納形式について説明する。図4はウィルスパターン格納手段11の格納形式を示す図である。ウィルスパターン格納手段11は、ウィルスパターンVPを検索テーブル11aと、シリアル番号保持情報11bとに分けて格納する。

【0033】検索テーブル11aは、階層木構造をとる。それぞれ木の深さに応じて第1次階層、第2次階層、第3次階層…と呼ぶ。また、それぞれの枝部分とシリアル番号を対応させておく。

【0034】シリアル番号保持情報11bは、現在自分の持っているシリアル番号とバージョンと脅威レベルを保持しており、ウィルスパターンVPのマルチキャストパケットが来た際、これと比較して変更が必要かどうかを判断する。

【0035】次に検索テーブル11aに新規にウィルスパケットVPを追加する場合の処理について説明する。各ウィルスチェックルータ10a～10nは、自分の保持しているウィルスパターンVPのシリアル番号と、バージョンとを比較し、その結果に基づいて検索テーブル11aに格納

【0036】マルチキャストによる新規のウィルスパターンVPから自分の担当分を受け取ると、ウィルスパターンVP情報を記録したシリアル番号保持情報11bをもとにウィルスパターンVPの検索テーブル11aを更新する。

【0037】まず、シリアル番号とバージョンをチェックして変更が必要か判断する。変更が必要と判断すると検索テーブル11aの第1次階層、第2次階層、…と比較して重ならない部分を探し、そこから新規に枝を伸ばす。その後、新規追加した枝を最上位に移動させ、登録を終了する。

【0038】図5はウィルスパターン格納手段11でのウィルスパターンVPを新規登録する際の処理手順を示すフローチャートである。

【S1】シリアル番号を自分のウィルスチェックルータ内持っているかどうかを判断する。持っている場合はステップS2へ、持っていない場合はステップS4へ行く。

【S2】バージョン更新かどうかを判断する。更新ならばステップS3へ、更新でなければ終了する。

【S3】対象のシリアル番号の枝を削除する。

【S4】第1次階層と比較する。ステップS4の詳細は図6で説明する。

【0039】図6は第n次階層と比較して、新たに枝を作成する際の処理手順を示すフローチャートである。

【S10】ウィルスパターンから1文字とる。

【S11】既存の検索テーブル11aの第n次階層と比較する。

【S12】ヒットした場合はステップS13へ、そうでなければステップS14へ行く。

【S13】次の第n+1次階層と比較する。

【S14】枝を追加する。

【S15】枝の優先順位を上にもってくる。

【0040】以上説明したような処理手順で、新規のウィルスパターンVPに対して対応する枝を作成していき格納しておく。次にウィルスチェックルータ10の構成について説明する。図7はウィルスチェックルータ10の構成を示す図である。

【0041】図に示す通常のバケットは、本発明のウィルスチェック手段12に該当するウィルスチェックフィルタ12でウィルスチェックが行われる。ここでウィルスチェックを行うべきバケットは、バケットの中身がTCPかつFTP、HTTP、SMTPのいずれかのバケットで、かつまだチェックが完了していないバケットである。

【0042】ただし、それ以外のバケットは、負荷軽減のためウィルスチェックフィルタ12をウィルスチェックせずに通過させる。また、オフセット値がある一定以上のバケットは、つまりフローの後ろのものをバケットと通

を立てる。

【0043】一方、マルチキャストのバケットは、シリアル番号保持情報11bでウィルスパターンの更新処理が行われ、検索テーブル11aに階層木構造形式で格納される。

【0044】そして、経路計算部13aで経路計算をした後、バケット生成送信部13bは、ウィルスチェックに引っかかったバケットに対して、後述のIPヘッダのオプションのフィールドにビットを立てた感染表示バケットPbを生成する。以降の同一のフローのバケットに対してもビットを立てる。

【0045】また、バケット生成送信部13bは、IPバケットの送信元に向けて警告バケットPw1を生成する。その後、感染表示バケットPb、警告バケットPw1を送信する。

【0046】なお、警戒モードに設定して、感染元との通信を遮断する警戒モード設定手段14については後述する。一方、クライアント端末20では、ソフトウェアによってIPヘッダのウィルス感染を示すビットを監視している。ビットが立った感染表示バケットPb及び警告バケットPw1を受け取ったクライアント端末20は、ユーザに対してウィルスに感染した旨のメッセージ表示を行う。

【0047】次にIPヘッダの構成について説明する。図8はIPヘッダの構成を示す図である。バージョンは4ビットで、インターネットヘッダの形式を示す。IH L (Internet Header Length)は4ビットで、ヘッダ長が32ビットワード単位で示される。サービスタイプは8ビットで、スループット等のサービス品質が示される。全長は16ビットで、オクテットで区切った長さを示す。なお、全長にはヘッダとデータを含む。

【0048】識別番号は16ビットで、送信側を識別するために割り当てられた値でデータグラムのフラグメントを組み立てる際に使用される。Flagは3ビットで、フラグメントの分割許可または継続等の制御を示す。フラグメントオフセットは13ビットで、データグラム内でフラグメントの占める位置を示す。

【0049】ttlは8ビットでデータグラムがインターネットのシステムに留まっていられる時間の最小値を示す。プロトコルは8ビットで、データグラムのデータ部を渡すべきトランスポートレイヤプロトコルを示す。ヘッダチェックサムは16ビットでヘッダに対するチェックサムを示す。

【0050】始点アドレスは32ビットで、始点のIPアドレスを示す。終点アドレスは32ビットで終点のIPアドレスを示す。オプションは可変長で、ユーザが任意に定義できる。本発明ではこのオプション領域を利用して感染表示バケットPb、警告バケットPw1及び

警告バケットPw1の生成をする

〔S21〕オフセット値が一定以上かどうかを判断する。一定以上の場合はステップS30へ、そうでなければステップS22へ行く。

〔S24〕感染しているかどうかを判断する。感染している場合はステップS28へ、そうでなければステップS25へ行く。

〔S27〕チェック済みのビットを立てる。

〔S29〕警告パケットPw1、警戒情報パケットPw2を発行する。

【0052】次に上記のステップS23のウイルスチェックルーティンについて説明する。バケット内の1バイトを取り、まず検索テーブル11a内の第1次階層と比較する。同じものがあつた場合は、バケットから次の1バイトを取り、一致した枝の配下の第2次階層と比較する。

【0053】もし当てはまらなくなったらパケットの次の1バイトを取り出して最初から比較をやり直す。これを繰り返し最後まで当てはまる場合は、このバイトはウイルスに感染したと判断しIPヘッダのオプションのフィールドのビットを立てる。

【0054】また、もし検索の途中でパケットが終了した場合は感染していないものとみなし、代わりに別の領域を担当しているウイルスチェックルーティンにまかせる。図10はウイルスチェックルーティンの処理手順を示すフローチャートである。

【S 4 1】パケット完了かどうかを判断する。パケット完了の場合は終了し、そうでなければステップS 4 2へ行く。

〔S43〕ヒットしたかどうかを判断する。ヒットした場合はフネツプC44へ、そうでなければフネツプC45へ

完了の場合はステップ S 49へ、そうでなければステップ S 48へ行く。

〔S 49〕 ウィルス感染と判断する。

【0055】次にウィルスチェック時に立てるビットについて説明する。ウィルスチェックルーチでウィルスチェックを実施すると、まずIHLフィールドを1増加してオプション領域を確保する。そして、確保されたオプション領域にビットを立てる。

【0056】図11は感染表示パケットPbのIPパケットのフォーマットを示す図である。まず、IHLフィールドを1増加する。そして、オプション領域をThe Copied flag=0、The option Classes=3(将来の予約用領域)、The option Number=1(感染表示パケットPb:ウィルスチェックをしたことを示すコード)、Length=5と設定する。

【0057】また、Option Valueとして第1ビットは第1領域チェック未/済、第2ビットは第2領域チェック未/済、第3ビットは第3領域チェック未/済と割り当てる。すなわち、ウィルスチェックをしたかどうかの情報を記す。

【0058】そして、第4ビットはウィルス未感染/感染を示し、未感染なら0、感染している場合は1を立てて、感染表示パケットPbを表す。なお、第5ビット以降はシリアル番号である。

【0059】次に警告パケット Pw1 について説明する。ウィルスチェックルータでウィルスを検知した際に送信元には警告パケット Pw1 を送信し、周囲のウィルスチェックルータには警戒情報パケット Pw2 をマルチキャストで送信する。これによってウィルスの早期発見、拡大防止をはかる。

【0060】警告バケットPw1は、ウィルス検知時のバケットと同様にIPヘッダのオプション領域のビットを立て、以下のフォーマットで送信元へ配送される。図12は警告バケットPw1のフォーマットを示す図である。まず、IHLLフィールドを1増加する。そして、オプション領域でThe Copied flag=0、The option class=es-3（将来の予約用領域）、The option Number=2（警告バケットPw1を示すコード）、Length=3と設定する。そして、図11で説明したチェック済/清のオプションを付加する。また、終点アドレスが感染元のアドレスとなる。

【0061】次にクライアント側の処理について説明する。図13はクライアント端末20の構成を示す図である。本発明の構成は、例えば、検査手帳21およびLANドライバ

ドライブ22bに含まれる。

【0062】LANDドライブ21aは、送られてくる各フローについて、各パケットのウィルスチェックビットを見る。そして、ビットが立っているかどうかを判断し、その結果をTCP/IPドライブ22bに通知する。

【0063】TCP/IPドライブ22bは、ビットが立っている旨の通知を受けると、対応するファイルを実行不可にした後、ファイルを削除する旨のメッセージ20-1を表示する。

【0064】次にクライアント端末20でのビット監視の流れについて説明する。図14、図15はクライアント端末20のビット監視の処理手順を示すフローチャートである。

【S50】パケットを読み込む。

【S51】新規のフローかどうかを判断する。新規のフローの場合はステップS52へ、そうでなければステップS53へ行く。

【S52】フロー情報を追加する。

【S53】終了フローかどうかを判断する。終了フローの場合はステップS54へ、そうでなければステップS55へ行く。

【S54】フロー情報から該当フローを削除する。

【S55】ビットをチェックする。

【S56】ヒットしたかどうかを判断する。ヒットした場合はステップS58へ、そうでなければステップS57へ行く。

【S57】TCP/IPドライブ22bに処理を渡す。

【S58】警告パケットPw1かどうかを判断する。警告パケットの場合はステップS59へ、そうでなければステップS60へ行く。

【S59】警告の旨のメッセージを表示する。

【S60】ファイルの実行権をなくす。

【S61】警告メッセージ20-1の表示を行う。

【0065】次に警戒情報パケットPw2について説明する。ウィルスチェックルータでウィルス検知された際、各ウィルスチェックルータにはマルチキャストで警戒情報パケットPw2を出す。警戒情報パケットPw2はウィルスパケットのシリアル番号と送信元IPアドレスを情報として持ち、マルチキャストで配布される。

【0066】警戒情報パケットPw2を受け取った各ウィルスチェックルータは受け取ったシリアル番号のウィルスパターンVPの検索の優先順位を上げる。図16は警戒情報パケットPw2のフォーマットを示す図である。警戒情報パケットPw2は、ヘッダPw2-1にEthernet HeaderとIP Header(Multicast)とを持つ。

【0067】そして、警戒情報を示すコードPw2-2と、ウィルスの種類を示すシリアル番号Pw2-3と、そのパケットのシリアル番号Pw2-4を持つ。その

と、ウィルス感染元のIPアドレスPw2-6をつける。

【0068】次に警戒情報パケットPw2を受け取った際の検索順序の処理手順について説明する。図17は警戒情報パケットPw2を受け取った際の検索順序の処理手順を示す図である。

【S70】警戒情報パケットPw2からシリアル番号を取得する。

【S71】第1次階層、第2次階層、…第n次階層、の検索順位を最上位に上げる。

【0069】次に感染元との通信遮断を行うための警戒モード設定手段14について説明する。脅威レベルがある一定以上の場合、拡大を防止するためウィルスチェックルータ側でホストとの通信を一定時間遮断させる。

【0070】警戒情報パケットPw2の中の脅威レベルを見て、ある一定以上の場合はIPアドレスをテーブルに保存し、警戒モードに移行する。警戒モードでは通常の処理の前になるパケットをチェックし、テーブルにあるアドレスから来たパケットと、テーブルにあるアドレスに向かうパケットと、を一定時間だけすべて廃棄する。

【0071】廃棄させる時間は、再送要求がタイムアウトする程度の時間とし、テーブルに保存された時にカウンタと一緒に設定される。もしこの時間内にパケットが来なかったらテーブルから削除し、警戒モードを解除する。逆にパケットが来たら時間(カウンタのカウンタ値)を延長させる。

【0072】図18は警戒モード設定手段14が行う警戒モードの処理手順を示すフローチャートである。

【S80】脅威レベルは一定以上かどうかを判断する。一定以上の場合は、ステップS81へ、そうでなければステップS89へ行く。

【S81】警戒IPアドレスを保持する警戒IPアドレステーブルにIPアドレスと、警戒モードにしておく時間をカウントするカウンタ値と、を設定する。

【S82】パケットを読み込む。

【S83】始点/終点のアドレスがテーブルと一致するかどうかを判断する。一致する場合はステップS84へ、そうでなければステップS86へ行く。

【S84】パケットを廃棄する。

【S85】カウンタ値を延長する。すなわち、警戒モードにする時間をさらに長くする。

【S86】カウンタ値を減少する。すなわち、警戒モードにする時間を短くする。

【S87】カウンタを終了するかどうかを判断する。終了の場合はステップS88へ、終了しない場合はステップS82へ戻る。

【S88】警戒IPアドレステーブルからIPアドレスレ

【0073】次にウイルスチェックルータの協調による負荷分散及びチェック精度向上について説明する。ウイルスのバイナリデータは小さく、パケットをまたがってバイナリが分割してしまう場合がある。したがって、各ウイルスチェックルータ毎に担当するウイルスパターンVPを異なるように分担させ保持させる。

【0074】これにより、もしある領域で仮りにパケットの途中でウイルスのバイナリが切れてしまった場合でも、別なパケットでは別の領域のチェックにかかるようになる。

【0075】ウイルスチェックルータに対するウイルスパターンの各分担は、手動でも自動でも設定可能とする。ただし、手動で設定する場合は、パケットは受信先に到着するまでにはすべての領域がチェックされるような構成、つまりそれぞれ分担しているウイルスチェックルータを最低1回ずつは通るような構成にする必要がある。

【0076】次に自動で設定する場合について説明する。図19は担当分担領域要求パケットのフォーマットを示す図である。図に示すフォーマットを用いて自動設定する。

【0077】まず、新規のウイルスチェックルータは担当分担領域要求パケット100を自分が配布可能な全てのウイルスチェックルータに配布する。この場合t1領域は小さく設定して、余計な負荷は極力かけないようにしておく必要がある。

【0078】また、自分が持つルーティング情報から自分の接続している全ウイルスチェックルータそれぞれに対して、終点アドレスを挿入したパケットを発行する。オプション領域は、The Copied flag=0、The option Classes=3 (将来の予約用領域)、The option Number=3 (担当分担領域要求パケット100を示すコード)、Length=3、「空き」と設定する。

【0079】この担当分担領域要求パケット100を受け取った各ウイルスチェックルータは、送信元に対して自分の担当領域を以下のような担当領域要求応答パケット101にのせて返送する。図20は担当分担領域要求応答パケット101のフォーマットを示す図である。

【0080】t1がまだ残っていれば、自分が受け取ったウイルスチェックルータ以外の配送できる範囲の全てのウイルスチェックルータに対して回報する。担当分担領域要求応答パケット101のオプション領域は、The Copied flag=0、The option Classes=3 (将来の予約用領域)、The option Number=4 (担当分担領域要求応答パケット101を示すコード)、Length=3、「担当領域」と設定する。

【0081】また、送信側のウイルスチェックルータは、返ってきた担当分担領域要求応答パケット101から各領域を担当するウイルスルータの名称を抽出し、各ルータに通知する。

る。

【0082】以上説明したように、本発明のウイルスチェックネットワーク1は、ウイルスチェックルータにウイルスチェック機能を搭載させることにより、ネットワーク側でウイルスを検知させることができ、ウイルス侵入防止をより多くのクライアントに対して、またより確実に行うことができる。

【0083】また、常に最新のウイルスパターン情報をウイルスチェックルータ間でマルチキャストにより交換通知し、またその更新方法もマルチキャストのパケットを発行するだけであるので、新たなウイルスへの対応が簡単にかつ迅速に行うことができる。またクライアント側で更新をかける必要がない。

【0084】さらに、検知したウイルスに対する警告を各ウイルスチェックルータが同時に行うことで早期発見、拡大防止を図る。そして、送信元に対してもし警告パケットを送ることでウイルス感染を通知することができる。

【0085】また、各ウイルスチェックルータでウイルスチェック領域を分担することで、各々ウイルスチェックルータにかかる負荷を分散することができ、フレーム間にまたがってウイルスが存在する場合においてもいずれかを担当しているウイルスチェックルータでチェックすることができ、ウイルスチェックの精度が向上する。

【0086】さらに、ウイルスが検知されたパケットを落とすことはせずに、IPヘッダにビットを立てて受信側に通知することで再送などによる余計なトラフィックの増加を防ぐことができる。そして、ウイルスの脅威レベルに応じて通信を遮断させるため、感染の拡大を防止させることができる。

【0087】

【発明の効果】以上説明したように、本発明のウイルスチェックネットワークは、複数のウイルスチェック装置を設けて、ネットワーク側でウイルスチェックを行う構成とした。これにより、ネットワーク側でウイルスを未然に防ぐことができるので、ウイルスの感染及び拡大を防止でき、ウイルスチェック対策効率の向上を図ることが可能になる。

【図面の簡単な説明】

【図1】本発明のウイルスチェックネットワークの原理図である。

【図2】ウイルスチェックルータを配置したネットワークの概要を示す図である。

【図3】ウイルスパターンVPのフォーマットを示す図である。

【図4】ウイルスパターンVP格納手段の格納形式を示す図である。

【図5】ウイルスパターン格納手段でのウイルスパターンバイナリを新規に格納する際の処理手順を示すフローチャートである。

【図6】第n次階層と比較して、新たに枝を作成する際の処理手順を示すフローチャートである。

【図7】ウィルスチェックルータの構成を示す図である。

【図8】IPヘッダの構成を示す図である。

【図9】ウィルスチェックの処理手順を示すフローチャートである。

【図10】ウィルスチェックルーティンの処理手順を示すフローチャートである。

【図11】感染表示パケットのIPパケットのフォーマットを示す図である。

【図12】警告パケットのフォーマットを示す図である。

【図13】クライアント端末の構成を示す図である。

【図14】クライアント端末のビット監視の処理手順を示すフローチャートである。

【図15】クライアント端末のビット監視の処理手順を示すフローチャートである。

【図16】警戒情報パケットのフォーマットを示す図である。

【図17】警戒情報パケットを受け取った際の検索順番*

*の処理手順を示す図である。

【図18】警戒モードの処理手順を示すフローチャートである。

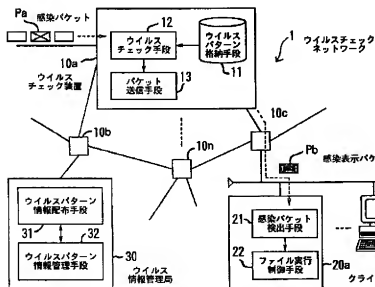
【図19】担当分担領域要求パケットのフォーマットを示す図である。

【図20】担当分担領域要求応答パケットのフォーマットを示す図である。

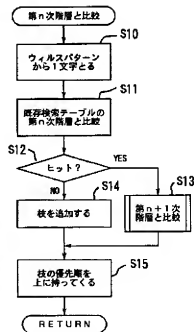
【符号の説明】

- 1 ウィルスチェックネットワーク
- 10a～10n ウィルスチェック装置
- 11 ウィルスパターン格納手段
- 12 ウィルスチェック手段
- 13 パケット送信手段
- 20a～20m クライアント端末
- 21 感染パケット検出手段
- 22 ファイル実行制御手段
- 30 ウィルス情報管理局
- 31 ウィルスパターン情報配布手段
- 32 ウィルスパターン情報管理手段
- Pa 感染パケット
- Pb 感染表示パケット

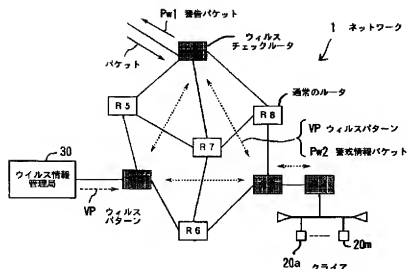
【図1】



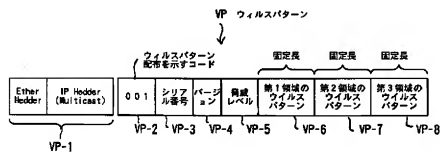
【図6】



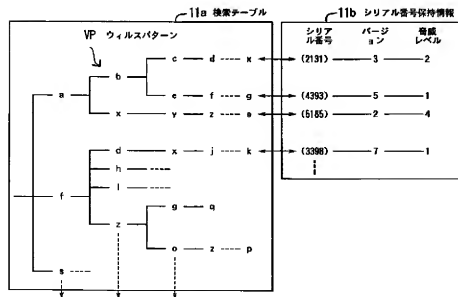
【図2】



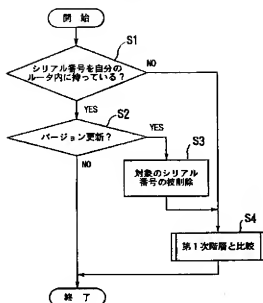
【図3】



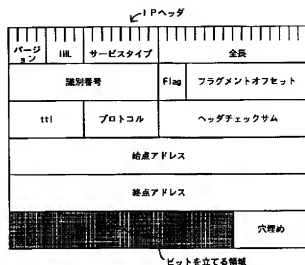
【図4】



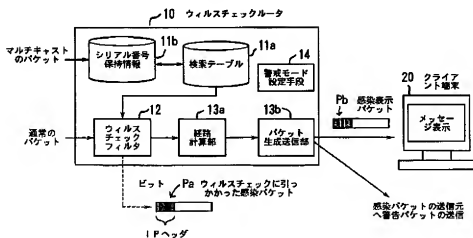
【図5】



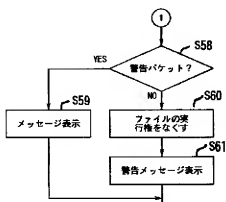
【図8】



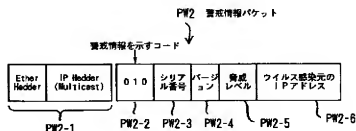
【図7】



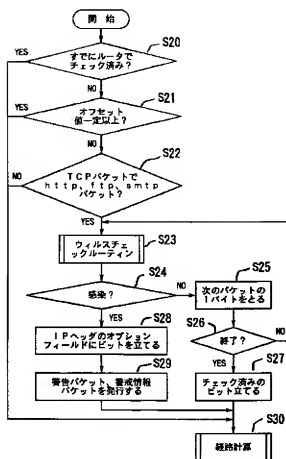
【図15】



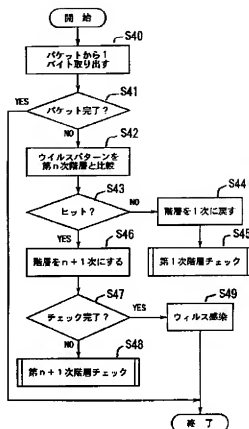
【図16】



【図9】

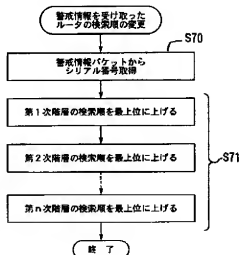
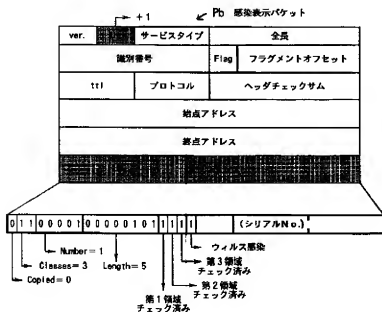


【図10】

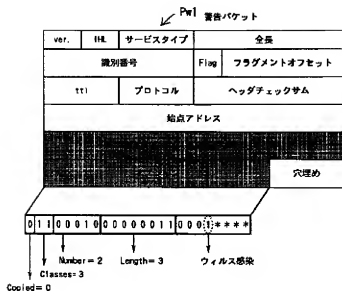


【図17】

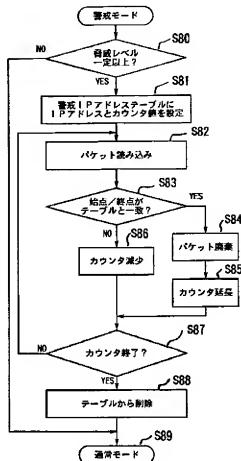
【図11】



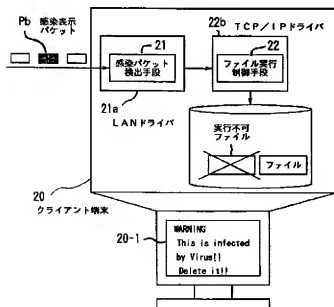
【図12】



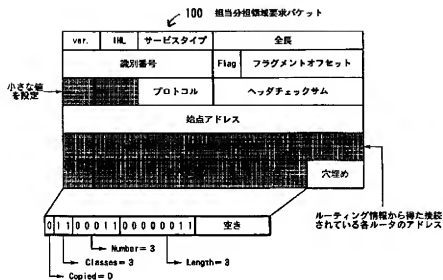
【図18】



【図13】



【図 19】



【図 20】

